Cloud Security for Government

**Business Challenges**

Increasingly, federal, state, and local governments look to cloud technologies to improve employee productivity and collaboration as well as save money. However, these institutions are held to the highest standards when it comes to compliance and legal regulations. In adopting cloud services, security considerations task government institutions with three primary imperatives:

**Comply with Regulations**

Government agencies must adhere closely to compliance mandates around a wide range of regulations, including protecting Personally Identifiable Information (PII), International Traffic in Arms Regulations (ITAR), Federal Information Security Management Act (FISMA).

**Protect Sensitive Data**

Government institutions hold a great deal of sensitive information, including the compliance-specific information described above, but also extending to typical business-related information sets, such as employee records, financials, and intellectual property. Ensuring that this information is properly controlled with the appropriate access and sharing permissions is essential to the vitality of the organization. At the same time, it is critical to avoid data breaches and the many negative side-effects they entail.

**Defend Against Cyber threats**

Given the many valuable information payloads residing within government agencies’ cloud environments, cyber criminals target government institutions with increasing frequency and persistence. To combat cyber threats, government agencies must be able to rapidly identify suspicious behavior and equip themselves with the tools to respond accordingly.

**Cisco cloud security: effective security made simple**

Cisco’s cloud offerings helps government organizations use and monitor cloud apps with Cisco Cloudlock, and proactively hunt threats that may pose a risk on your network and valuable data with Investigate. The Cisco cloud security suite enables consistent security policies and enforcement, up-to-date threat intelligence, greater scalability, and improved performance. The result: government agencies are able to foster a productive and collaborative environment, all while maintaining a highly secure and compliant environment.
Cisco Cloudlock

Cisco Cloudlock is the cloud-native Cloud Access Security Broker (CASB) that helps accelerate use of the cloud. Cisco Cloudlock secures your cloud identities, data, and apps, while enabling compliance and improving productivity.

Cisco Cloudlock is a simple, open, and automated solution that combats cloud account compromises, data breaches and cloud app ecosystem risks, by providing actionable cybersecurity intelligence. Cisco Cloudlock orchestrates existing security investments to provide a coordinated, best-of-breed security solution.

Cisco Umbrella Investigate

Cisco Umbrella Investigate provides threat intelligence about domains, IPs, autonomous systems (ASNs), and file hashes across the internet. Security teams — including incident responders, security operations specialists, and threat hunters — can leverage Investigate’s web-based console or API to quickly glean live threat intelligence on a particular indicator of compromise (IOC). By pivoting between different data points in Investigate, security teams can expand their view of an attacker’s infrastructure and speed up incident response.

Investigate leverages a massive, diverse dataset of 120+ billion daily DNS requests from our global users and live views of the network connections from our 600+ BGP peering partners. We then apply statistical and machine learning models to the data to automatically uncover patterns and predict future malicious places on the internet.

Key Benefits

Defend against cyber threats

- Cisco Cloudlock provides protection against account compromise with cross-platform User and Entity Behavior Analytics (UEBA). Cloudlock also detects activities outside of whitelisted countries and actions performed across distances in an impossible amount of time.

- Adopt a more proactive security posture by leveraging Investigate’s complete view of the relationships between domains, networks, and malware to pinpoint where the next attack is being staged.

Manage compliance in the cloud

- With Cisco Cloudlock, enforce compliance through out-of-the-box policies designed for PCI-DSS, SOX, and other compliance-specific information & tailor policies to proprietary concerns, such as intellectual property through our highly-configurable policy engine.

Enrich existing security investments

- Increase the value of IDaaS solutions to complement Cisco Cloudlock’s User and Entity Behavior Analytics with automated response actions such as requiring multi-factor authentication, restricting application access, and reducing maximum session length. Also, aggregate on-premises logs with Cisco Cloudlock app risk insight for superior Shadow IT visibility.

- Leverage Investigate’s API to enrich your SIEM or other security system with our global threat intelligence and to help prioritize incident response.

Protect sensitive information

- Cisco Cloudlock can pinpoint excessively exposed sensitive information within cloud environments based on defined content or exposure criteria & users can enforce automated, contextual policy-driven response actions.

- For a security team that needs more context around an IOC, tap into Investigate to hunt threat actors and gain insight into malicious internet infrastructure.